KnowBe4

Kevin Mitnick's Top 15 Tips for Defenders

1 New-school security awareness training for your users is critical to inoculate them against phishing attacks and social engineering.

2 Inventory all computer-related devices in the business to create an updated network topology map, which is a high-level overview of the network. The map should detail all network flows through gateways, routers, and firewalls, as well as indicate the external and internal IP addresses of these devices.

3 Implement proper password management using best security practices like password managers for users, and privileged password management tools for admins.

4 Patching is critical for both internal and external workstations and servers. **Do NOT forget to patch/upgrade firmware on firewall, routers, and IoT devices.** What you don't patch may come back to bite you.

5 Disable Link-Local Multicast Name Resolution (LLMNR), WPAD, and NBT-NS (NetBIOS name service) to mitigate responder attacks. These protocols are commonly abused to conduct NTLM relay attacks and impersonate hosts to steal NTLMv2 hashes that could potentially be cracked offline.

6 Disable Windows Spool Service on Domain Controllers and Exchange Servers unless needed for business purposes. This mitigates the printer bug used with NTLM relay attacks.

7 Configure Microsoft LAPS to manage local administrator passwords.

8 Install Little Snitch on all MacOS clients and upgrade to Catalina for better security mitigations.

9 Test how easy it may be for a threat-actor to compromise your internal network to obtain Domain Admin rights. The best tool to analyze the easiest path an attacker can take is: https://github.com/BloodHoundAD/Bloodhound/wiki

10 Configure and enable logging on your systems. Please see, https://www.malwarearchaeology.com/cheat-sheets

11 Log all events to your favorite SIEM and refine alerts (yes, write your own detections if possible) based on events that may flag suspicious behaviors. This should be in addition to your EDR (Endpoint Detection & Response) tools.

12 Enable Two-Factor Authentication (2FA) on all external reachable devices such as VPNs and servers. Moreover, enable 2FA on all cloud services like O365, G-Suite, AWS, Azure, etc.

13 Check your users' passwords to ensure they are not included in one or more of the numerous data breaches. KnowBe4's free Password Exposure Test runs an in-depth analysis of your organization's hidden exposure risk associated with your users - https://www.knowbe4.com/password-exposure-test

14 Harden Active Directory against malicious attacks. Please check out https://adsecurity.org

15 It's highly recommended that your company conduct an annual penetration test covering at minimum, the company's internal and external network, internet-facing web applications, and your employee's susceptibility to sophisticated social engineering attacks.

KnowBe4
Human error. Conquered.
33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com